ALBANIAN JOURNAL
OF MATHEMATICS
Volume 4, Number 4, Pages 147–160
ISSN 1930-1235: (2010)

SINGULAR LOCUS ON THE SPACE OF GENUS 2 CURVES WITH DECOMPOSABLE JACOBIANS.

LUBJANA BESHAJ

Abstract. We study the singular locus on the algebraic surface $\mathfrak{S}_n$ of genus 2 curves with a (n,n)-split Jacobian. Such surface was computed by Shaska in [15] for $n=3$, and Shaska at al. in [3] for $n=5$. We show that the singular locus for $n=2$ is exactly th locus of the curves of automorphism group D_4 or D_6. For $n=3$ we use a birational parametrization of the surface $\mathfrak{S}_3$ discovered in [15] to show that the singular locus is a 0-dimensional subvariety consisting exactly of three genus 2 curves (up to isomorphism) which have automorphism group D_4 or D_6. We further show that the birational parametrization used in $\mathfrak{S}_3$ would work for all $n \geq 7$ if $\mathfrak{S}_n$ is a rational surface.

1. Introduction

We study the singular locus on the space of genus 2 curves with a (n,n)-split Jacobian. Such curves have been of much interest lately because of their use in many theoretical and applicative situations. The first part of the paper is based on several papers on the topic of genus two curves with split Jacobians; see [1,3–9,11–14,16–21] among others.

In the first section, we study genus 2 curves with split Jacobian. Let $\mathcal{X}$ be a genus 2 curve defined over an algebraically closed field k, of characteristic zero. Let $\psi : \mathcal{X} \to E$ be a degree n maximal covering (i.e. does not factor through an isogeny) to an elliptic curve E defined over k. We say that $\mathcal{X}$ has a degree n elliptic subcover. Degree n elliptic subcovers occur in pairs. Let $(E; E')$ be such a pair. It is well known that there is an isogeny of degree n^2 between the Jacobian Jac $(\mathcal{X})$ of $\mathcal{X}$ and the product $E \times E'$. We say that $\mathcal{X}$ has (n,n)-split Jacobian.

The locus of genus two curves with (n,n)-split Jacobians is an irreducible 2-dimensional algebraic variety. There are many descriptions of it in the literature, but throughout this paper we will use only the embdedding of such space in the moduli space $\mathcal{M}_2$. In other words, we would like an equation of such space where every point corresponds precisely to one isomorphism class of genus 2 curves. We denote such surface by $\mathfrak{S}_n$ and always think of it given by an equation in terms of the absolute invariants i_1, i_2, i_3 of genus two curves; see [21]. We will call the surface $\mathfrak{S}_n$ the Shaska surface of level n.

The case with $(3,3)$-split Jacobian was studied in [15]. These are the curves with degree 3 elliptic subcovers. Shaska in [15] computed the locus of curves $\mathcal{X}$

2010 *Mathematics Subject Classification.* 14Q15, 14Q05, 68W30.
Key words and phrases. genus two curves, moduli spaces, hyperelliptic curve cryptography, modular polynomials.

with degree 3 elliptic subfield in the moduli space of genus 2 curves. We will give the explicit equation of this space and also a graphical representation of it. It was the first time that such an equation was computed other than the computationally trivial case for $n = 2$.

In [3] was studied the case with $(5, 5)$ - split Jacobian by Shaska, Magaard, and Voelklein. There was computed a normal form for the curves in the locus $\mathfrak{S}_5$ and its three distinguished subloci. Further, they have computed the equation of the elliptic subcover in all cases, gave a birational parametrization of the subloci of $\mathfrak{S}_5$ as subvarieties of $\mathcal{M}_2$ and classify all curves in these loci which have extra automorphisms.

In section 2 of this paper we compute the singular locus, $\mathcal{T}_2$, of the space $\mathfrak{S}_2$, and the singular locus $\mathcal{T}_3$ of the space $\mathfrak{S}_3$. The definition of the singular locus depends on the parametrization of the surface. For the case of $n = 2$ we prove that the singular locus of $\mathfrak{S}_2$ is exactly the locus of genus 2 curves with automorphism group D_4 or D_6. This computations were done using Maple 14.

If the surface $\mathfrak{S}_n$ is rational then we show how to obtain a birational parametrization for $\mathfrak{S}_n$ using the invariants of binary cubics, which were used first in [15].

Throughout this paper by a genus two curve we mean the isomorphism class of a genus two curve defined over an algebraically closed field k. While most of the results are true for most characteristics, we assume throughout that the characteristic of k is zero.

2. Preliminaries

2.1. **Genus 2 curves with split Jacobian.** Let $\mathcal{X}$ be a genus 2 curve defined over an algebraically closed field k, of characteristic zero. The affine version of this curve is given by the equation $\mathcal{X} : y^2 = F(x)$, where $F(x)$ is a polynomial of degree 5 or 6 and discriminant different from zero. Let

$$\psi : \mathcal{X} \to E$$

be a degree n covering, where n is odd and E is an elliptic curve. The degree n covering $\psi : \mathcal{X} \to E$ induces a degree n cover $\phi : \mathbb{P}^1 \to \mathbb{P}^1$ such that the following diagram commutes.

$$\begin{tikzcd} & \mathcal{X} \arrow[dl, "\psi"'] \arrow[dr, "\pi_1"] & \\ E \arrow[dr, "\pi_2"'] & & \mathbb{P}^1 \arrow[dl, "\phi"] \\ & \mathbb{P}^1 & \end{tikzcd}$$

Here, $\pi_1 : \mathcal{X} \to \mathbb{P}_1$ and $\pi_2 : E \to \mathbb{P}_2$ are the hyperelliptic projections. So, $\phi \circ \pi_1 = \pi_2 \circ \psi$. From Riemann- Hurwitz formula the number of branch points is 4, or 5. The ramification of the function ϕ is as follows; there are $\frac{n-1}{2}$ points of index 2 in q_1, q_2 and q_3, and $\frac{n-3}{2}$ points of index 2 in q_4, and there is only one point of index 2 in q_5. We denote this type of ramification by

$$\left((2)^{\frac{n-1}{2}}, (2)^{\frac{n-1}{2}}, (2)^{\frac{n-1}{2}}, (2)^{\frac{n-3}{2}}, (2) \right).$$

In the following figure bullets (resp., circles) represent places of ramification index 2 (resp., 1).

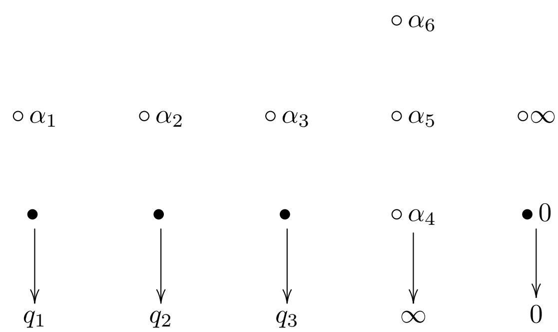

FIGURE 1. Ramification of $\phi : \mathbb{P}^1 \to \mathbb{P}^1$ when $n = 3$

The family of coverings $\phi : \mathbb{P}^1 \to \mathbb{P}^1$, is an irreducible 2-dimensional algebraic variety. For every ϕ there exists a genus 2 curve C. Let $\mathcal{H}$ be the family of coverings. We have the map

$$\alpha : \mathcal{H} \to \mathcal{M}_2$$
$$[\phi] \to [\mathcal{X}]$$

Let $\alpha(\mathcal{H})$ be denoted by $\mathfrak{S}_n$. So, we say that these curves $\mathcal{X}$ are parametrized by an irreducible 2-dimensional subvariety $\mathfrak{S}_n$ of the moduli space $\mathcal{M}_2$ of genus 2 curves. The fact that $\mathfrak{S}_n$ is irreducible, for n odd, comes from the braid action on Nielsen classes. It is known that this is the case for all $n \cong 1 \mod 2$; see [20] among others. Computation of spaces $\mathfrak{S}_n$ as a subvariety of $\mathcal{M}_2$ has first computed by Shaska in [15] for $n = 3$ and then by Shaska, Magaard, and Voelklein for $n = 5$; see [3]. We will call the space $\alpha(\mathcal{H}) \hookrightarrow \mathcal{M}_2$ the **Shaska surface of level** n.

2.2. **Pairs of elliptic subcovers.** Let $\psi_1 : \mathcal{X} \longrightarrow E_1$ be a covering of degree n from a curve of genus 2 to an elliptic curve. The covering $\psi_1 : \mathcal{X} \longrightarrow E_1$ is called a **maximal covering** if it does not factor over a nontrivial isogeny. A map of algebraic curves $f : X \to Y$ induces maps between their Jacobians $f^* : J_Y \to J_X$ and $f_* : J_X \to J_Y$. When f is maximal then f^* is injective and $ker(f_*)$ is connected, see [20] for details.

Let $\psi_1 : \mathcal{X} \longrightarrow E_1$ be a covering as above which is maximal. Then ${\psi^*}_1 : E_1 \to J_C$ is injective and the kernel of $\psi_{1,*} : J_{\mathcal{X}} \to E_1$ is an elliptic curve which we denote by E_2, see [17] or [21]. For a fixed Weierstrass point $P \in C$, we can embed C to its Jacobian via

$$i_P : \mathcal{X} \longrightarrow J_C$$
$$x \to [(x) - (P)]$$

Let $g : E_2 \to J_C$ be the natural embedding of E_2 in J_C, then there exists $g_* : J_{\mathcal{X}} \to E_2$. Define $\psi_2 = g_* \circ i_P : \mathcal{X} \to E_2$. So we have the following exact sequence

$$0 \to E_2 \xrightarrow{g} J_{\mathcal{X}} \xrightarrow{\psi_{1,*}} E_1 \to 0$$

The dual sequence is also exact, see [20]

$$0 \to E_1 \xrightarrow{\psi_1^*} J_{\mathcal{X}} \xrightarrow{g_*} E_2 \to 0$$

The following lemma shows that ψ_2 has the same degree as ψ_1 and is maximal.

$$\begin{tikzcd} & \mathcal{X} \arrow[dl, "\psi_1"'] \arrow[dr, "\psi_2"] & \\ E_1 & & E_2 \end{tikzcd}$$

FIGURE 2. Splitting of the genus two curve

Lemma 1. *a) deg* $(\psi_2) = n$
b) ψ_2 *is maximal*

For the proof see [20]. If $deg(\psi_1)$ is an odd number then the maximal covering $\psi_2 : \mathcal{X} \to E_2$ is unique (up to isomorphism of elliptic curves).

To each of the covers $\psi_i : \mathcal{X} \longrightarrow E_i$, $i = 1, 2$, correspond covers $\phi_i : \mathbb{P}^1 \longrightarrow \mathbb{P}^1$. If the cover $\psi_1 : \mathcal{X} \longrightarrow E_1$ is given, and therefore ϕ_1, we want to determine $\psi_2 : \mathcal{X} \longrightarrow E_2$ and ϕ_2. The study of the relation between the ramification structures of ϕ_1 and ϕ_2 provides information in this direction. The following lemma answers this question for the set of Weierstrass points $W = \{P_1, \dots, P_6\}$ of $\mathcal{X}$ when the degree of the cover is odd.

Let $\psi_i : \mathcal{X} \longrightarrow E_i$, $i = 1, 2$, be maximal of odd degree n. Let $\mathcal{O}_i \in E_i[2]$ be the points which has three Weierstrass points in its fiber. Then, we have the following:

Lemma 2. *The sets* $\psi_1^{-1}(\mathcal{O}_1) \cap W$ *and* $\psi_2^{-1}(\mathcal{O}_2) \cap W$ *form a disjoint union of W.*

Thus, the elliptic subcovers occur in pairs.

2.3. **Describing the Shaska surface $\mathfrak{S}_n$ in $\mathcal{M}_2$.** Consider a genus two curve $\mathcal{X}$ defined over k, given with equation

$$\mathcal{X} : \quad y^2 = a_6 X^6 + a_5 X^5 + \cdots + a_0.$$

Igusa J-invariants $\{J_{2i}\}$ of $\mathcal{X}$ are homogeneous polynomials of degree $2i$ in

$$k[a_0, \dots, a_6], \ \textit{for } i = 1, 2, 3, 5;$$

see [21], [10] for their definitions. Here J_{10} is simply the discriminant of $f(X, Z)$. These J_{2i} are invariant under the natural action of $SL_2(k)$ on sextics. Dividing such an invariant by another one of the same degree gives an invariant under $GL_2(k)$ action.

Two genus 2 fields K (resp., curves) in the standard form $Y^2 = f(X, 1)$ are isomorphic if and only if the corresponding sextics are $GL_2(k)$ conjugate. Thus if I is a $GL_2(k)$ invariant (resp., homogeneous $SL_2(k)$ invariant), then the expression $I(K)$ (resp., the condition $I(K) = 0$) is well defined. Thus the $GL_2(k)$ invariants are functions on the moduli space $\mathcal{M}_2$ of genus 2 curves. This $\mathcal{M}_2$ is an affine variety with coordinate ring

$$k[\mathcal{M}_2] = k[a_0, \dots, a_6, J_{10}^{-1}]^{GL_2(k)}$$

which is the subring of degree 0 elements in $k[J_2, \dots, J_{10}, J_{10}^{-1}]$. The *absolute invariants*

$$i_1 := 144 \frac{J_4}{J_2^2}, \ i_2 := -1728 \frac{J_2 J_4 - 3 J_6}{J_2^3}, \ i_3 := 486 \frac{J_{10}}{J_2^5},$$

are even $GL_2(k)$-invariants. Two genus 2 curves with $J_2 \neq 0$ are isomorphic if and only if they have the same absolute invariants. If $J_2 = 0$ then we can define new

invariants as in [21]. For the rest of this paper if we say "there is a genus 2 curve $\mathcal{X}$ defined over k" we will mean the k-isomorphism class of $\mathcal{X}$.

Remark 1. *The definitions of i_1, i_2, i_3 with J_2 in the denominator is done simply for computational purposes.*

Let

$$F(X) = a_3 X^3 + a_2 X^2 + a_1 X + a_0, \ \ and\ G(X) = b_3 X^3 + b_2 X^2 + b_1 X + b_0$$

be two cubic polynomials. We define the following invariants

$$H(F, G) := a_3 b_0 - \frac{1}{3} a_2 b_1 + \frac{1}{3} a_1 b_2 - a_0 b_3$$

We denote by $R(F, G)$ the resultant of F and G and by $D(F)$ the discriminant of F always with respect to X. Also,

$$r_1(F, G) = \frac{H(F, G)^3}{R(F, G)}, \quad r_2(F, G) = \frac{H(F, G)^4}{D(F)\, D(G)}.$$

In [2] it is shown that r_1, r_2, and $r_3 = \frac{H(F,G)^2}{J_2(F\, G)}$ form a complete system of invariants for unordered pairs of cubics.

Every curve $\mathcal{X}$ in $\mathfrak{S}_n$ is written as a product of two cubics. In other words, its equation is

$$y^2 = F(X) \cdot G(X)$$

for some $F(X), G(X) \in k[X]$. We will use the invariants r_1, r_2 in relation with these cubics. Since the discriminants of such cubics can not be zero (otherwise the curve is not a genus two curve) then $D(F), D(G)$ are nonzero. For the same reason $F(X)$ and $G(X)$ don't have any common factors. Hence, $R(F, G) \neq 0$. Thus, r_1, r_2 are everywhere defined.

3. Computation of singular locus $\mathcal{T}_n$

Throughout this section we will use x, y, z for absolute invariants i_1, i_2, i_3 respectively. Let $\mathfrak{S}_n$ be the Shaska surface of level n given by

$$\mathfrak{S}_n(x, y, z) = 0$$

Then, its singular set is defined as the solution of the system

$$\begin{cases} \dfrac{\partial \mathfrak{S}_n}{\partial x} = 0 \\ \dfrac{\partial \mathfrak{S}_n}{\partial x} = 0 \\ \dfrac{\partial \mathfrak{S}_n}{\partial x} = 0 \\ \mathfrak{S}_n(x, y, z) = 0 \end{cases} \tag{1}$$

3.1. **The singular locus $\mathcal{T}_2$.** The equation of $\mathfrak{S}_2$ is given by

$$\begin{aligned} \mathfrak{S}_2(x, y, z) = & -27\, x^6 - 9459597312000\, z^2\, x^2 + 20639121408000\, z^2\, y + 111451255603200\, z^2\, x - 240734712102912\, z^2 \\ & - 55240704\, z\, x^4 - 18\, y^2\, x^4 - 8294400\, z\, y^2\, x^2 - 47278080\, z\, y\, x^3 - 2641807540224000000\, z^3 \\ & - 2866544640000\, z^2\, y\, x + 2\, x^6\, y - 4\, x^3\, y^3 + 9\, x^7 + 331776\, z\, x^5 + 107495424\, z\, y\, x^2 - 27\, y^4 + 9\, x\, y^4 \\ & - 52254720\, z\, y^2\, x + 2\, y^5 + 161243136\, z\, y^2 + 161243136\, z\, x^3 - 12441600\, z\, y^3 + 54\, x^3\, y^2 = 0 \end{aligned}$$

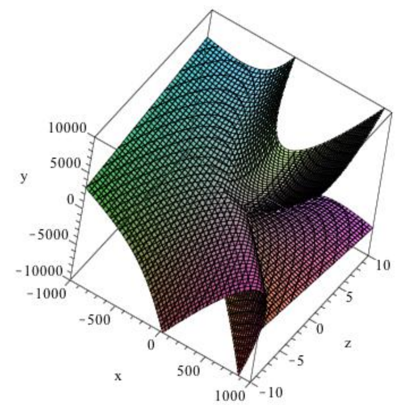

FIGURE 3. The surface $\mathfrak{S}_2$ graphed in $\mathbb{R}^3$.

Then we have the corresponding system from which we eliminate z and get

$$z = -\frac{1}{82944}\,\frac{\phi_1(x,y)}{\phi_2(x,y)}$$

where ϕ_1 and ϕ_2 are as follows;

$$\begin{aligned}\phi_1(x,y) &= 104976\,y^2 + 5211\,x^5 - 48600\,y^2x + 69984\,yx^2 + 3375\,yx^4 + 450\,x^3y^2\\ &\quad - 50544\,x^4 - 675\,x^2y^2 + 104976\,x^3 + 2025\,xy^3 - 10800\,y^3 + 20\,x^6 + 250\,y^4\\ &\quad - 37800\,x^3y\\ \phi_2(x,y) &= 1250\,yx^2 - 121500\,xy - 3779136 - 359100\,x^2 - 11250\,y^2 + 6375\,x^3\\ &\quad + 421200\,y + 2274480\,x\end{aligned}$$

The locus $\mathcal{T}_2$ which has 3 irreducible components which we describe below algebraically and graphically.

The first component is given by

$$C_1: \quad 100\,y^2 - 1458\,y + 540\,xy - 243\,x^2 + 80\,x^3 = 0$$

it corresponds to the locus of genus two curves with automorphism group D_4.

The second component is given by

$$C_2: 3888\,x - 1188\,x^2 + 5\,x^3 + 432\,y - 360\,xy - 25\,y^2 = 0$$

and it corresponds to the locus of genus two curves with automorphism group D_6.

The third component of $\mathcal{T}_2$ is given by the following system

$$C_3: \quad \begin{cases} 50\,x^4 - 7515\,x^3 - 825\,yx^2 + 20412\,x^2 - 23490\,xy - 4050\,y^2 + 52488\,y = 0\\ 125\,y^2 - 1620\,y + 1125\,xy - 5832\,x + 1890\,x^2 + 25\,x^3 = 0\end{cases}$$

The solution of the C_3 system is

$$\begin{cases} y = \dfrac{1}{75}\,\dfrac{408240\,x - 33525\,x^2 - 944784 + 250\,x^3}{-864 + 55\,x}\\ 125\,x^3 - 9450\,x^2 + 247860\,x - 944784 = 0\end{cases}$$

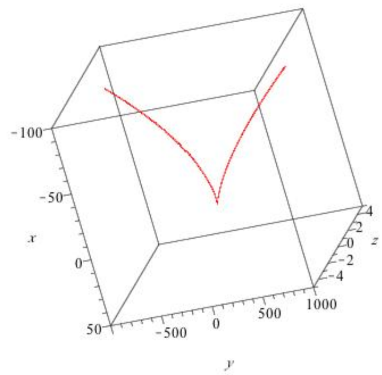

FIGURE 4. The component C_1

and the points (x, y) given by

$$\left(0, \frac{729}{50}\right), \left(\frac{81}{20}, -\frac{729}{200},\right), \left(-\frac{36}{5}, \frac{1512}{25}\right)$$

However, only the first point is on the variety and it is

$$\left(0, \frac{729}{50}, \frac{729}{12800000}\right)$$

and has automorphism groups are D_4 and therefore is contained in the first component.

We summarize in the following theorem:

Theorem 1. *The singular locus of $\mathcal{T}_2$ contains two components, the irreducible loci of curves of automorphism group D_4 and D_6.*

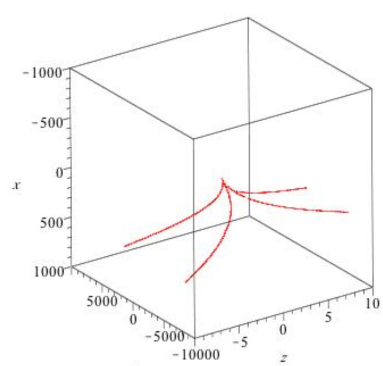

FIGURE 5. The component C_2

3.2. **The locus $\mathcal{T}_3$.** In this section we compute the singular locus $\mathcal{T}_3$ of $\mathfrak{S}_3$. The equation of $\mathfrak{S}_3$ is quite large and was computed in [15]. Below we display this equation $\mathfrak{S}(x, y, z) \mod 5$.

$$
\begin{aligned}
&x^{20} + 3\,x^{19} + 3\,x^{18}y + 4\,x^{17}y^2 + 3\,x^{18} + 4\,x^{17}z + 2\,x^{16}y^2 + 2\,x^{16}yz + 2\,x^{15}y^3 + 4\,x^{16}z + 2\,x^{15}y^2 \\
&+ 4\,x^{15}yz + x^{15}z^2 + x^{13}y^3z + 3\,x^{14}yz + x^{13}y^2z + x^{13}yz^2 + 4\,x^{12}y^3z + 4\,x^{12}y^2z^2 + x^{11}y^4z + x^{10}y^5z \\
&+ 4\,x^{13}z^2 + x^{12}y^2z + 4\,x^{12}z^3 + 3\,x^{11}y^3z + 3\,x^{11}y^2z^2 + 2\,x^{11}yz^3 + 4\,x^{10}y^4z + 2\,x^{10}y^3z^2 \\
&+ 2\,x^9y^5z + 2\,x^9y^4z^2 + 2\,x^8y^6z + x^7y^7z + 4\,x^5y^{10} + 3\,x^{12}z^2 + 3\,x^{11}yz^2 + 3\,x^{11}z^3 + 4\,x^{10}yz^3 + 4\,x^9y^4z \\
&+ 3\,x^9y^3z^2 + 2\,x^9y^2z^3 + 3\,x^8y^5z + 4\,x^8y^4z^2 + 3\,x^8y^3z^3 + 2\,x^7y^6z + 2\,x^7y^5z^2 + 3\,x^5y^8z + 2\,x^4y^{10} + x^4y^9z \\
&+ 2\,x^3y^{11} + x^2y^{12} + 2\,x^{10}z^3 + 3\,x^9y^2z^2 + 4\,x^9yz^3 + x^9z^4 + 4\,x^8y^3z^2 + 4\,x^8y^2z^3 + 2\,x^8yz^4 + 3\,x^7y^4z^2 \\
&+ 2\,x^6y^6z + 4\,x^6y^5z^2 + 2\,x^6y^4z^3 + 3\,x^5y^7z + x^5y^5z^3 + 4\,x^4y^7z^2 + 2\,x^3y^{10} + 3\,x^3y^9z + 4\,x^3y^8z^2 + 3\,xy^{12} \\
&+ 4\,xy^{11}z + 3\,y^{13} + 4\,x^9z^3 + x^8yz^3 + 3\,x^8z^4 + 2\,x^7y^2z^3 + 2\,x^7yz^4 + 2\,x^7z^5 + x^6y^4z^2 + x^6y^3z^3 + 3\,x^6y^2z^4 \\
&+ x^6yz^5 + 4\,x^5y^5z^2 + x^5y^4z^3 + x^5y^3z^4 + x^4y^6z^2 + 2\,x^4y^5z^3 + x^4y^4z^4 + 3\,x^3y^6z^3 + 3\,x^2y^9z + 3\,x^2y^8z^2 \\
&+ 4\,x^2y^7z^3 + 4\,xy^{10}z + 3\,y^{12} + 2\,y^{11}z + x^7z^4 + x^6y^2z^3 + 3\,x^6yz^4 + 3\,x^6z^5 + 4\,x^5y^3z^3 + x^5y^2z^4 + 3\,x^5yz^5 \\
&+ 3\,x^5z^6 + 2\,x^4y^4z^3 + 4\,x^4y^3z^4 + x^4y^2z^5 + 4\,x^3y^4z^4 + 3\,x^3y^3z^5 + 2\,x^2y^7z^2 + 4\,x^2y^6z^3 + 2\,x^2y^5z^4 \\
&+ 2\,xy^8z^2 + 3\,xy^7z^3 + 3\,y^{10}z + 3\,y^9z^2 + 2\,x^6z^4 + 3\,x^5yz^4 + 3\,x^5z^5 + x^4y^2z^4 + 3\,x^4z^6 + 2\,x^3y^3z^4 \\
&+ 3\,x^3y^2z^5 + 3\,x^2y^5z^3 + 3\,x^2y^4z^4 + 3\,xy^6z^3 + 2\,xy^5z^4 + 2\,xy^4z^5 + 2\,y^7z^3 + y^5z^5 + 2\,x^4z^5 + x^3yz^5 \\
&+ 3\,x^3z^6 + 2\,x^2y^3z^4 + 2\,x^2y^2z^5 + 2\,x^2yz^6 + 2\,xy^4z^4 + 3\,y^5z^4 + 4\,y^4z^5 + 2\,x^3z^5 + 3\,x^2yz^5 + 4\,x^2z^6 + xy^2z^5 \\
&+ 3\,y^2z^6 + xz^6 + 3\,y^2z^5 + 4\,z^7 + 3\,z^6 = 0
\end{aligned}
$$

Let $\mathcal{X}$ be a genus 2 curve in the locus $\mathfrak{S}_3$. Then, $\mathcal{X}$ is given by the equation

$$
y^2 = (4x^3v^2 + x^2v^2 + 2xv + 1)(x^3v^2 + x^2uv + xv + 1), \tag{2}
$$

see [19] for details. In [15] was computed the equation of $\mathfrak{S}_3$ using the map

$$
\theta : (u, v) \to (i_1, i_2, i_3)
$$

where the absolute invariants i_1, i_2, i_3 in terms of u, v are

(3)

$$
\begin{aligned}
i_1 =& \frac{144}{v(-405 + 252u + 4u^2 - 54v - 12uv + 3v^2)^2}(1188u^3 - 8424uv + u^4v - 24u^4 \\
&+ 14580v - 66u^3v + 138uv^2 + 297u^2v + 945v^2 - 36v^3 + 9u^2v^2) \\
i_2 =& -\frac{864}{v^2(-405 + 252u + 4u^2 - 54v - 12uv + 3v^2)^3}(-81v^3u^4 + 2u^6v^2 + 234u^5v^2 \\
&+ 3162402uv^2 - 21384v^3u + 26676v^4 - 473121v^3 - 72u^6v - 5832v^4u + 14850v^3u^2 \\
&- 72v^3u^3 + 324v^4u^2 - 650268u^3v - 5940u^3v^2 - 3346110v^2 + 432u^6 - 1350u^4v^2 \\
&+ 136080u^4v - 7020u^5v - 307638u^2v^2 \\
i_3 =& -243\frac{(v - 27)(4u^3 - u^2v - 18uv + 4v^2 + 27v)^3}{v^3(-405 + 252u + 4u^2 - 54v - 12uv + 3v^2)^5}
\end{aligned}
$$

The map

$$
\theta : (u, v) \to (i_1, i_2, i_3)
$$

given by (3) which has degree 2 and it is defined when $J_2 \neq 0$. For now we assume that $J_2 \neq 0$ (The case $J_2 = 0$ is treated in Section 4.2, of [15]). Denote the minors of the Jacobian matrix of θ by $M_1(u, v), M_2(u, v), M_3(u, v)$. The solutions of

$$
\begin{cases} M_1(u,v) = 0 \\ M_2(u,v) = 0 \\ M_3(u,v) = 0 \end{cases} \tag{4}
$$

consist of the (non-singular) curve

$$
8v^3 + 27v^2 - 54uv^2 - u^2v^2 + 108u^2v + 4u^3v - 108u^3 = 0 \tag{5}
$$

and 7 isolated solutions which we display in Table 1, together with the corresponding values (i_1, i_2, i_3), the automorphism group, and the number of elliptic subcovers.

(u,v)	(i_1, i_2, i_3)	$Aut(K)$	$e_3(K)$
$(-\frac{7}{2}, 2)$	$J_{10} = 0$, no associated genus 2 field K		
$(-\frac{775}{8}, \frac{125}{96})$, $(\frac{25}{2}, \frac{250}{9})$	$-\frac{8019}{20}, -\frac{1240029}{200}, \frac{531441}{100000}$	D_4	2
$(27 - \frac{77}{2}\sqrt{-1}, 23 + \frac{77}{9}\sqrt{-1})$, $(27 + \frac{77}{2}\sqrt{-1}, 23 - \frac{77}{9}\sqrt{-1})$	$(\frac{729}{2116}, \frac{1240029}{97336}, \frac{531441}{13181630464}$	D_4	2
$(-15 + \frac{35}{8}\sqrt{5}, \frac{25}{2} + \frac{35}{6}\sqrt{5})$, $(-15 - \frac{35}{8}\sqrt{5}, \frac{25}{2} - \frac{35}{6}\sqrt{5})$	$81, -\frac{5103}{25}, -\frac{729}{12500}$	D_6	2

TABLE 1. Exceptional points where det $(Jac(\theta)) = 0$

Notice that the curve given by Eq. (5) corresponds to genus 2 curves with isomorphic degree 3 elliptic subcovers. Hence, the cover has singular branch locus on such cases. We will see next how this can be avoided when we use the invariants of a pair of cubics.

3.3. **Birational parametrization of $\mathfrak{S}_3$.** For $F(X) = (4x^3v^2 + x^2v^2 + 2xv + 1)$ and $G(X) = (x^3v^2 + x^2uv + xv + 1)$ we have

$$
\begin{aligned}
r_1(F,G) &= 27\frac{v(v-9-2u)^3}{4v^2 - 18uv + 27v - u^2v + 4u^3} \\
r_2(F,G) &= -1296\frac{v(v-9-2u)^4}{(v-27)(4v^2 - 18uv + 27v - u^2v + 4u^3)}
\end{aligned} \tag{6}
$$

Lemma 3. *The function field of $\mathfrak{S}_3$ is given by $k(r_1, r_2)$. In other words $k(i_1, i_2, i_3) = k(r_1, r_2)$. Moreover;*

(7)

$$
\begin{aligned}
i_1 &= \frac{9}{4}\frac{(13824r_1^3r_2^2 + 442368r_1^2r_2^3 + 5308416r_1r_2^4 + 192r_1^4r_2 + r_1^5 + 786432r_1r_2^3 + 9437184r_2^4)}{r_1(-1152r_2^2 + 96r_2r_1 + r_1^2)^2} \\
i_2 &= \frac{27}{8r_1^2(-1152r_2^2 + 96r_2r_1 + r_1^2)^3}(+79626240r_1^4r_2^4 - 4076863488r_1^2r_2^5 + 34560r_1^6r_2^2 \\
&\quad + 12230590464r_1^2r_2^6 + 32614907904r_1r_2^6 + 14495514624r_2^6 + 288r_1^7r_2 + 2211840r_1^5r_2^3 \\
&\quad + r_1^8 - 212336640r_1^3r_2^4 + 1528823808r_1^3r_2^5 - 2359296r_1^4r_2^3) \\
i_3 &= -521838526464\frac{r_2^9}{r_1^2(-1152r_2^2 + 96r_2r_1 + r_1^2)^5}
\end{aligned}
$$

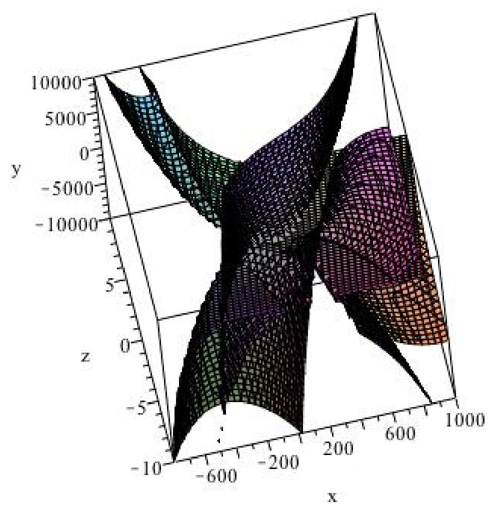

FIGURE 6. Shaska surface $\mathfrak{S}_3$

The solution of the system in

$$
\begin{cases} M_1(r_1, r_2) = 0 \\ M_2(r_1, r_2) = 0 \\ M_3(r_1, r_2) = 0 \end{cases} \tag{8}
$$

is

$$
-1152r_2^2 + 96r_1r_2 + r_1^2 = 0 \tag{9}
$$

and the system

$$
\begin{cases}
3\,{r_1}^8 + 720\,{r_1}^7 r_2 + 69120\,{r_1}^6 {r_2}^2 + 2048\,{r_1}^5 {r_2}^2 + 3317760\,{r_1}^5 {r_2}^3 + 79626240\,{r_1}^4 {r_2}^4 - 417792\,{r_1}^4 {r_2}^3 \\
\quad - 24772608\,{r_1}^3 {r_2}^4 + 764411904\,{r_1}^3 {r_2}^5 - 113246208\,{r_1}^2 {r_2}^5 + 50331648\,r_1 {r_2}^5 \\
\quad - 5435817984\,r_1 {r_2}^6 - 2415919104\,{r_2}^6 = 0 \\
9\,{r_1}^5 + 1296\,{r_1}^4 r_2 + 62208\,{r_1}^3 {r_2}^2 - 10240\,{r_1}^2 {r_2}^2 + 995328\,{r_1}^2 {r_2}^3 + 786432\,r_1 {r_2}^3 - 2359296\,{r_2}^4 = 0 \\
9\,{r_1}^8 + 2160\,{r_1}^7 r_2 + 207360\,{r_1}^6 {r_2}^2 + 9953280\,{r_1}^5 {r_2}^3 + 38912\,{r_1}^5 {r_2}^2 + 238878720\,{r_1}^4 {r_2}^4 \\
\quad - 3735552\,{r_1}^4 {r_2}^3 + 2293235712\,{r_1}^3 {r_2}^5 - 247726080\,{r_1}^3 {r_2}^4 + 905969664\,{r_1}^2 {r_2}^5 \\
\quad + 201326592\,r_1 {r_2}^5 - 5435817984\,r_1 {r_2}^6 - 4831838208\,{r_2}^6 = 0
\end{cases}
$$

Then we get the following singular points

$$
(r_1, r_2) = \left(-\frac{512}{2187}, -\frac{256}{6561}\right), \left(\frac{2}{243}, \frac{1}{11664}\right), \left(-\frac{4000}{2187}, \frac{2500}{6561}\right)
$$

and the corresponding points (respectively) in $\mathfrak{S}_3$ are:

$$
\begin{aligned}
(i_1, i_2, i_3) = &\left(-\frac{8019}{20}, -\frac{1240029}{200}, -\frac{531441}{100000}\right), \\
&\left(81, -\frac{5103}{25}, -\frac{729}{12500}\right), \\
&\left(\frac{729}{2116}, \frac{1240029}{97336}, \frac{531441}{13181630464}\right)
\end{aligned}
$$

which have automorphism groups respectively D_4, D_4, D_6, as seen from Table 1.

Notice that the Eq. (9) is exactly the case for $J_2 = 0$ where i_1, i_2, i_3 are not defined.

Corollary 1. *The singular locus $\mathcal{T}_3$ of $\mathfrak{S}_3$ are the points*

$$
\left(-\frac{8019}{20}, -\frac{1240029}{200}, -\frac{531441}{100000}\right), \left(81, -\frac{5103}{25}, -\frac{729}{12500}\right), \left(\frac{729}{2116}, \frac{1240029}{97336}, \frac{531441}{13181630464}\right)
$$

which have automorphisms group D_4, D_4, D_6 respectively.

Notice that we have to use a parametrization in order to get the singular locus, because it is difficult computationally to compute this locus via partial derivatives.

4. Some remarks for the general case.

Let's give a general approach how one can attempt to compute the surface $\mathfrak{S}_n$ for $n \geq 7$. For $n \geq 7$ we get the first general case where the symmetries between the fourth and the fifth branch points which occur for degree 5 do not occur any longer; see [3].

Suppose that $n \geq 7$. Then $\mathfrak{S}_n$ is parametrized by the r_1, r_2 invariants of two cubics. As in [20] we write a system of equations for the degree 7 covering $\phi : \mathbb{P}^1 \to \mathbb{P}^1$.

Let $\mathcal{X}$ be a genus 2 curve in $\mathfrak{S}_n$ which has equation

$$
y^2 = (x^3 + ax^2 + bx + c)\,(x^3 + ux^2 + vx + w)
$$

such that a, b, c, u, v are expressed in terms of the two parameters u and v. Let r_1 and r_2 be the invariants of the two cubics. Then, there is a birational parametrization of $\mathfrak{S}_n$ in terms of parameters (r_1, r_2), i.e.

$$
(r_1, r_2) \to (i_1, i_2, i_3)
$$

such that $k(\mathfrak{S}_n) = k(r_1, r_2)$. Moreover, the singular locus of this parametrization contains the locus

$$J_2(r_1, r_2) = 0$$

While the computation of $\mathfrak{S}_n$ for $n \geq 7$ is more difficult because the degree is larger, it is also true that there are no other symmetries now other than the S_3 action on the first three branch points as described in [15] and [3] for cases $n = 3, 5$ respectively.

Acknowledgements: I would like to thank the Department of Mathematics at Oakland University for their support during the time that this article was written.

References

[1] L. Beshaj and T. Shaska, *The arithmetic of genus two curves*, Algebraic aspects of digital communications, NATO Sci. Peace Secur. Ser. D Inf. Commun. Secur., vol. 25, IOS, Amsterdam, 2011, pp. to appear.

[2] V. Krishnamoorthy, T. Shaska, and H. Völklein, *Invariants of binary forms*, Progress in Galois theory, Dev. Math., vol. 12, Springer, New York, 2005, pp. 101–122, DOI 10.1007/0-387-23534-5-6, (to appear in print). MR2148462 (2006b:13015)

[3] K. Magaard, T. Shaska, and H. Völklein, *Genus 2 curves that admit a degree 5 map to an elliptic curve*, Forum Math. **21** (2009), no. 3, 547–566, DOI 10.1515/FORUM.2009.027. MR2526800 (2010h:14050)

[4] K. Magaard, T. Shaska, S. Shpectorov, and H. Völklein, *The locus of curves with prescribed automorphism group*, Sūrikaisekikenkyūsho Kōkyūroku **1267** (2002), 112–141. Communications in arithmetic fundamental groups (Kyoto, 1999/2001). MR1954371

[5] N. Pjero, M. Ramasaço, and T. Shaska, *Degree even coverings of elliptic curves by genus 2 curves*, Albanian J. Math. **2** (2008), no. 3, 241–248. MR2492097 (2010b:14058)

[6] E. Previato, T. Shaska, and G. S. Wijesiri, *Thetanulls of cyclic curves of small genus*, Albanian J. Math. **1** (2007), no. 4, 253–270. MR2367218 (2008k:14066)

[7] R. Sanjeewa and T. Shaska, *Determining equations of families of cyclic curves*, Albanian J. Math. **2** (2008), no. 3, 199–213. MR2492096 (2010d:14043)

[8] T. Shaska and V. Ustimenko, *On the homogeneous algebraic graphs of large girth and their applications*, Linear Algebra Appl. **430** (2009), no. 7, 1826–1837, DOI 10.1016/j.laa.2008.08.023. MR2494667 (2010a:05103)

[9] ———, *On some applications of graphs to cryptography and turbocoding*, Albanian J. Math. **2** (2008), no. 3, 249–255. MR2495815 (2010a:05102)

[10] T. Shaska and H. Völklein, *Elliptic subfields and automorphisms of genus 2 function fields*, Algebra, arithmetic and geometry with applications (West Lafayette, IN, 2000), Springer, Berlin, 2004, pp. 703–723. MR2037120 (2004m:14047)

[11] T. Shaska, G. S. Wijesiri, S. Wolf, and L. Woodland, *Degree 4 coverings of elliptic curves by genus 2 curves*, Albanian J. Math. **2** (2008), no. 4, 307–318. MR2470579 (2010b:14064)

[12] T. Shaska and G. S. Wijesiri, *Codes over rings of size four, Hermitian lattices, and corresponding theta functions*, Proc. Amer. Math. Soc. **136** (2008), no. 3, 849–857 (electronic), DOI 10.1090/S0002-9939-07-09152-6. MR2361856 (2008m:11132)

[13] ———, *Theta functions and algebraic curves with automorphisms*, Algebraic aspects of digital communications, NATO Sci. Peace Secur. Ser. D Inf. Commun. Secur., vol. 24, IOS, Amsterdam, 2009, pp. 193–237. MR2605301

[14] T. Shaska, C. Shor, and S. Wijesiri, *Codes over rings of size p^2 and lattices over imaginary quadratic fields*, Finite Fields Appl. **16** (2010), no. 2, 75–87, DOI 10.1016/j.ffa.2010.01.005. MR2594505 (2011b:94059)

[15] T. Shaska, *Genus 2 fields with degree 3 elliptic subfields*, Forum Math. **16** (2004), no. 2, 263–280, DOI 10.1515/form.2004.013. MR2039100 (2004m:11097)

[16] ———, *Some special families of hyperelliptic curves*, J. Algebra Appl. **3** (2004), no. 1, 75–89, DOI 10.1142/S0219498804000745. MR2047637 (2005i:14028)

[17] ———, *Computational aspects of hyperelliptic curves*, Computer mathematics, Lecture Notes Ser. Comput., vol. 10, World Sci. Publ., River Edge, NJ, 2003, pp. 248–257. MR2061839 (2005h:14073)

[18] ———, *Some open problems in computational algebraic geometry*, Albanian J. Math. **1** (2007), no. 4, 297–319. MR2367221 (2008k:14108)

[19] ———, *Genus 2 curves with* $(3,3)$*-split Jacobian and large automorphism group*, Algorithmic number theory (Sydney, 2002), Lecture Notes in Comput. Sci., vol. 2369, Springer, Berlin, 2002, pp. 205–218, DOI 10.1007/3-540-45455-1-17, (to appear in print). MR2041085 (2005e:14048)

[20] ———, *Curves of genus 2 with* (N,N) *decomposable Jacobians*, J. Symbolic Comput. **31** (2001), no. 5, 603–617, DOI 10.1006/jsco.2001.0439. MR1828706 (2002m:14023)

[21] ———, *Genus two curves covering elliptic curves: a computational approach*, Computational aspects of algebraic curves, Lecture Notes Ser. Comput., vol. 13, World Sci. Publ., Hackensack, NJ, 2005, pp. 206–231, DOI 10.1142/9789812701640-0013, (to appear in print). MR2182041 (2006g:14051)

Lubjana Beshaj, Department of Mathematics, University of Vlora, Albania.
E-mail address: `lbeshaj@univlora.edu.al`